IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JANE DOE, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED, Plaintiff, vs. AVID LIFE MEDIA, INC., and AVID DATING LIFE, INC. dba ASHLEY MADISON, Defendants.	Case No.: **COMPLAINT FOR DAMAGES, INJUNCTIVE RELIEF AND RESTITUTION** CLASS ACTION **JURY TRIAL DEMANDED**

Plaintiff JANE DOE ("Plaintiff"), individually and on behalf of herself and all other persons similarly situated, by her undersigned attorneys, alleges in this Complaint the following upon knowledge with respect to each of their own acts, and upon facts obtained through an investigation conducted by her counsel, which included, *inter alia*: (a) review and analysis of defendants' public documents and statements relevant to the instant action; (b) review and analysis of the marketing materials utilized by defendant in connection with the marketing and sales of the products subject of the Complaint; (c) information readily obtainable on the Internet; and (d) interviews of witnesses with personal knowledge of the relevant facts.

Plaintiff believes that further substantial evidentiary support will exist for the allegations set forth herein after a reasonable opportunity for discovery. Additional facts supporting the allegations contained herein are known only to defendant or are exclusively within its control.

I. NATURE OF THE ACTION

1. This is a class action arising from the deceptive marketing practices and insufficient means of securing the personally identifiable information of its customers by Defendants in operating the online dating site Ashley Madison.[1] This action is brought on behalf of a class consisting of all persons who registered for the website Ashley Madison, made purchases from Ashely Madison, or purchased the option to have their profile deleted from Ashley Madison for the maximum period permitted by the statute of limitation applicable to each of the claims through July 15, 2015 (the "Class Period") seeking to recover damages caused by defendants' unlawful conduct and violations of various state consumer protection laws (the "Class").

2. Ashley Madison is a website through which Defendants offer for use and sale a means by which consumers can attempt to procure personal relationships of various purposes with other users of the website. In particular, Defendants marketed Ashley Madison as a means through which consumers, citizens throughout the United States and this forum, who are in committed personal relationships can procure emotional and/or physical affairs with others members of the website. According to Defendants, "Ashley Madison is the most famous name in infidelity and married dating."

3. In order to provide its services to consumers, Ashley Madison solicits extensive personal information from its customers during and after the registration process. Such information included name, mailing address, date of birth, email address, password, and sensitive information pertaining to the sexual preferences and desires of the users. For users wishing to

[1] Defendants operate the Ashley Madison website by directing consumers to connect to computer servers it owns and operates through the universal resource locator (URL), commonly referred to as website address ashleymadison.com.

make purchases in order to make full use of the Ashley Madison website, such as having instant messaging online chats or sending messages to prospective matches, consumers were required to provide their credit card information, name, address, and telephone number.[2]

4. During the Class Period, Plaintiff and members of the Class provided the Personally Identifiable Information to Defendants, and Defendants retained said information in databases stored on computer servers under their control.

5. Due to the sensitive nature of the website and information that a consumer was required to share, Defendants marketed to consumers that its network system and the servers that contained consumers PII were equipped and monitored with the highest levels of security and date theft prevention to ensure that the PII would not be obtained by third parties attempting to circumvent Defendants' systems to acquire said PII. Defendants intended for this marketing information to entice consumers into registering on Ashley Madison and utilizing the website. Defendants further marketed to registered users the option to have their profile and information deleted from Defendants servers so that there would be no trace of the user that could later disclose their participation on Ashley Madison. This option was given a self-explanatory name: "Full Delete Removal." Defendants charged users $19 (nineteen dollars) to purchase this option.

6. Plaintiff and members of the Class relied upon the marketing materials developed and published by Defendants concerning the security measures of the Ashley Madison website, and the safety of their PII, in deciding to register on the website and purchase the services offered by Defendants. Plaintiff and members of the Class further purchased the Full Delete Removal option upon the belief that it would accomplish what its name expressly states – a full delete and removal of their PII and traces of their usage of Ashley Madison.

[2] Collectively, this information is referred to as "Personally Identifiable Information" or PII, throughout the complaint.

7. Defendants' marketing ploys were extremely successful. According to Defendants, Ashley Madison has approximately 37 million registered users. It is ranked by visits among the top 500 websites in the world, top 30 amongst adult websites, and had as many as 124.5 million visits in June 2015.[3] Defendant Avid Life Media, Inc. ("Avid Life Media")[4] grossed $115 million for 2014, an increase of 45% from the $78 million it grossed in 2013, netting the company pretax profits of $55 million.

8. On July 12, 2015, Defendants learned that their databases and computer systems had been compromised by a third party. On July 19, 2015, a third party calling themselves the "Impact Team" announced that it had hacked into the Ashley Madison servers and downloaded the PII of all of the users of Ashley Madison (the "Data Breach").

9. Rather than promptly inform members of the Class of the data breach, Defendants responded by misrepresenting when they learned of the breach, downplaying the breach and providing a false sense of security to those Class members that happened upon the news through third party sources. On July 20, 2015, Defendant Avid Life Media issued an update on its website stating that "our team has now successfully removed the posts related to this incident as well as all Personally Identifiable Information (PII) about our users published online."

10. To the astonishment and dismay of the Class, the truth was far from that presented by Defendants in their July 20, 2015 response. With its announcement, the Impact Team had contemporaneously demanded that if Defendants did not shut down Ashley Madison the Impact Team would release the user database. Defendants failed to disclose such in their July 20, 2015 announcement, and also failed to subsequently counter-act the demands of the Impact Team. On

[3] http://www.similarweb.com/website/ashleymadison.com (last visited August 26, 2015)
[4] Avid Life Media owns a handful of other dating sites including CougarLife.com and Establishedmen.com. Ashleymadison.com is by far the largest contributor to the company's earnings and profits.

August 18, 2015, the Impact Team released for public downloading and access the Ashley Madison user database containing the PII of the members of the Class. The Impact Team has also subsequently released damning correspondence and internal documents from Defendants evidencing Defendants' awareness of the weakness of the security systems it had in place to protect the Class' PII.

11. Along with the release of the PII, members of the Class who purchased the Full Delete Removal option from Ashley Madison (the "Full Delete Removal Subclass") learned for the first time that the Full Delete Removal had been misrepresented to them and the Full Delete Removal purchase did not provide what was marketed and promised – rather than delete in its entirety the PII and additional traces of users registration with Ashley Madison, the Full Delete Removal option merely deleted some limited profile data. Sufficient information concerning the identity of past users that had purchased the Full Delete Removal option remained stored on Ashely Madison's servers and the users' identities and participation on Ashely Madison were left for all to see in the data dumped by the Impact Team. Had members of the Full Delete Removal Sub-Class been aware that the Full Delete Removal service did not completely eliminate the traces of their past registration and use of Ashley Madison they would not have purchased the Full Delete Removal option.

12. Although Defendants had learned of the breach by at least July 19, 2015, Defendants did not make any adequate or prompt attempt to inform Plaintiff or the Class of the Data Breach. Finally, on August 19, 2015, Avid Life Media issued an update on its website merely indicating that it had "learned that the individual or individuals responsible for this attack claim to have released more of the stolen data." Defendants have not offered members of the Class any curative protection to assist the Class in preventing, addressing or curing the theft of

users PII or attempts to extort users with the wide spread disclosure of the sensitive information contained in the database.

13. The security breach, and the failure to promptly discover and block the Data Breach, was the result of Defendants' grossly inadequate information systems and security oversight. These failures enabled the perpetrators to obtain Class members' PII and subsequently use this information to steal from and extort members of the Class. Defendants' failures further put the Class members at serious risk of ongoing financial loss and identity theft, exposed the most sensitive, and embarrassing, information concerning their private lives to the world at large, and created irreparable harm.

14. While Defendants were enriched by its scheme through the monies it received from touting falsely the strength of its network security and the purported benefits of its "Full Delete" option, Plaintiff and the Class suffered damages as a result of each of their purchases of the Ashley Madison services because: (a) the services were not accompanied by the data security measures implied and expressly marketed by Defendants; (b) the information provided to Defendants necessary to obtain the services was not protected by the data security measures implied and expressly marketed by Defendants; (c) their private data was exposed so that it could be transferred and viewed by unauthorized third parties; (d) their PII, including users' addresses, phone number, email addresses and intimate preferences and practices, have been compromised and widely distributed publicly for the world to see creating irreparable harm; (e) they are exposed to a substantial risk of identity theft and related fraud; and (f) for the Full Delete Removal Subclass, the "Full Delete Removal" option and service did not provide the benefits implied and expressly marketed by Defendants.

15. Plaintiff and members of the Class were harmed by their registration for and acquisition of services offered by Defendants by being denied the value of what was marketed to Plaintiff and the Class.

16. Had Plaintiff and the Class members known of the true facts about Ashley Madison and the Full Delete Removal option they would either have not registered and made purchases from Ashley Madison, or would have not purchased the Products at inflated prices.

II. JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). The matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000, at least one member of the class of Plaintiff is a citizen of a state different from defendants, and the number of members of the proposed class is in the aggregate 100 or more.

18. This Court also has subject matter jurisdiction over the federal claims in this action pursuant to 28 U.S.C. § 1331.

19. This Court also has subject matter jurisdiction over the state law claims in this action pursuant to 28 U.S.C. § 1367(a) because they are so related to the federal claims so as to form part of the same case or controversy under Article III of the United States Constitution.

20. Exercise of jurisdiction over Defendants complies with the traditional notions of fair play and substantial justice as the Defendants purposefully availed themselves of the jurisdiction of this Court and reasonably foresaw that they would be subject of a lawsuit in this jurisdiction as a result of their marketing and directing the sales of the Services into this District and through the residence and/or significant and pervasive contacts with this District that gave rise to the present claims.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 in that many of the acts and transactions giving rise to this action occurred in this District, the actions giving rise to this action caused damages to Plaintiff and a substantial number of members of the Class within this district and because Defendants:

a. are authorized to conduct business in this district and has intentionally availed itself of the laws and markets within this district through the promotion, marketing, distribution and sale of its products in this district;

b. Does substantial business in this district; and

c. is subject to personal jurisdiction in this district.

III. PARTIES

22. Plaintiff Jane Doe (a pseudonym) was at all relevant times an adult female domiciled in New York County, New York.

23. At all relevant times herein, Plaintiff was exposed to and saw Defendants' claims and marketing concerning Ashley Madison and its protection of Plaintiff's PII. Particularly, in the making of her purchases, Plaintiff saw and relied upon the marketing materials concerning Ashley Madison and its protection of Plaintiff's PII. Unbeknownst to Plaintiff, Ashley Madison, as a result of Defendants' conduct and policies, had insufficient network and data security policies and implementations, and had failed to properly secure Plaintiff's PIIs. As a result Plaintiff did not receive the full value of the services marketed by Defendants, had her PII compromised as a result of Defendant's security failures and was, accordingly harmed through her purchases and use of the Ashley Madison website and services as alleged herein.

24. Defendant Avid Life Media is a corporation organized and existing under the laws of Ontario, Canada, and maintains its principal place of business in Toronto, Canada. Defendant

Avid Life Media owns and operates various companies that operate online dating websites including the website operated under the trademark of Ashley Madison.

25. Defendant Avid Dating Life, Inc. d/b/a Ashley Madison is a corporation organized and existing under the laws of Ontario, Canada, and maintains its principal place of business in Toronto, Canada. Defendant Avid Dating Life owns and operates online dating websites including the website operated under the trademark of Ashley Madison.

IV. FACTUAL ALLEGATIONS

26. Ashley Madison is an online dating site marketed as a service through which those in committed personal relationship can procure emotional and/or physical affairs with someone outside the committed personal relationship. According to Defendants, "Ashley Madison is the most famous name in infidelity and married dating," and "the most successful website for finding an affair and cheating partners." Defendants represent that "[t]housands of cheating wives and cheating husbands signup everyday looking for an affair" and offers.

27. According to Defendants, Ashley Madison has approximately 37 million registered users. It markets itself through advertisements on the internet, in print and on television. It is ranked by visits among the top 500 websites in the world, top 30 amongst adult websites, and had as many as 124.5 million visits in June 2015.[5] Ashley Madison substantially contributed to the $115 million in gross revenue for Defendant Avid Life Media in 2014, resulting in pretax profits of $55 million.

28. Ashley Madison's revenue model relies upon the purchase of "credits" by users that are used to interact with one another, as opposed to a subscription based model. Various means of interacting with other users, such as having instant messaging online chats or sending

[55] http://www.similarweb.com/website/ashleymadison.com (last visited August 26, 2015)

messages to prospective matches, will cost differing amount of credits. Defendants also generated revenue by capitalizing monetarily on the privacy and security concerns of Plaintiff and the Class by offering a $19 for-pay option that purported to delete the users' PII along with traces that could indicate that they are, or at one time were, members of Ashley Madison.

29. In order to provide its services to consumers, Ashley Madison solicits extensive personal information from its customers during and after the registration process. Such information included name, mailing address, date of birth, email address, user name, password, and sensitive information pertaining to the sexual preferences and desires of the users. For users wishing to make purchases on Ashley Madison, such as credits or the Full Delete option, users were required to provide their credit card information, name, address, and telephone number.

30. Defendants stored the PII on servers it controlled so as to provide services to Ashley Madison. Unbeknownst to Plaintiff and members of the Class, Defendants also stored and used some of the PII for their own use in order to analyze its users PII to enhance the service offerings of current users and marketing to prospective users.

31. During the Class Period, Plaintiff and members of the Class registered with Ashley Madison, provided their PII to Defendants via the Ashely Madison website, and Defendants retained said information in databases stored on computer servers under their control. In addition, Plaintiff and members of the Class provided their financial information and required PII to purchase "credits" from Defendants for use on the Ashley Madison website.

32. Due to the sensitive nature of the website and information that a consumer was required to share, Defendants marketed to consumers that its network system and the servers that contained consumers PII were equipped and monitored with the highest levels of security and date theft prevention to ensure that the PII would not be obtained by third parties attempting to

circumvent Defendants' systems to acquire said PII. Among these representations are labels on the Ashley Madison homepage indicating "100% Discreet Service," "Trusted Security Award," and an "SSL Secure Site." Defendants further frequently marketed the heightened security measures taken by making such statements that Ashley Madison is "the last truly secure space on the Internet."

33. Defendants intended for this marketing information to entice consumers into registering on Ashley Madison and utilizing the website. Defendants further marketed to registered users the option to have their profile and information deleted from Defendants servers so that there would be no trace of the user that could later disclose their participation on Ashley Madison. This option was given a self-explanatory name: "Full Delete." Defendants charged users $19 (nineteen dollars) to purchase this option.

34. Plaintiff and members of the Class relied upon the marketing materials developed and published by Defendants concerning the security measures of the Ashley Madison website, and the safety of their PII, in deciding to register on the website and purchase the services offered by Defendants. Plaintiff and members of the Class further purchased the Full Delete Removal option upon the belief that it would accomplish what its name expressly states – a full delete and removal of their PII and traces of their usage of Ashley Madison.

35. Unbeknownst to Plaintiff and the Class, Defendants misrepresented the extent and quality of the data security instituted to protect Ashley Madison's database and Plaintiff and the Class' PII. In reality, the Ashely Madison database lacked even the bare means of protection that should be applied to a sensitive database – encryption. Instead, the Plaintiff's and the Class members' PII was stored in an unencrypted format which would permit any unauthorized party who downloaded the database to view the contents unfettered.

36. Defendants were aware of severe security vulnerabilities in Ashley Madison. In an email dated May 15, 2015, between Ashley Madison's Director of Security Mark Steele to Ashley Madison's founder and chief executive officer, Mark Steele stated, in part:

> Our codebase has many (riddled?) XSS/CRSF vulnerabilities which are relatively easy to find (for a security researcher), and somewhat difficult to exploit in the wild (requires phishing). Other vulnerabilities would be things like SQL injection/data leaks, which would be much more damaging" [links added].

37. Defendants' active monitoring of its systems, a critically important aspect of data and network security, was wholly inadequate. According to an interview given by the Hacking Team, "[w]e were in Avid Life Media a long time to understand and get everything . . . [N]obody was watching. No security." Internally, there was "nothing to bypass . . . . [y]ou could use Pass1234 from the internet to VPN to root on all servers." In other words, Defendants internally frequently used a simple password "Pass1234" to allow anyone from the internet to get inside their virtual private network and thereafter gain access to the servers with unlimited authority. The hackers were, accordingly, able to extract and transfer outside of Defendants' network a massive amount of data - nearly 300 gigabytes.

38. On July 12, 2015, Defendants became aware that their computer systems had been accessed by unauthorized third parties. Defendants were made aware of this as the third party hacker installed a greeting screen on each of their employees' internal computers that greeted the employee with a message stating that Defendants had been hacked. Included in the on-screen message was the statement that "[w]e have taken over all systems in your entire office and production domains, all customer information databases, source code repositories, financial records, emails." Defendants remained silent as to this fact and subsequently misrepresented that they learned of the hack on July 20, 2015. The true timing of Defendants' discovery was disclosed only by the police during a press conference in August 24, 2015.

39. On or about July 19, 2015, a third party calling themselves the "Impact Team" issued an announcement online that it had hacked into the Ashley Madison servers and downloaded the PII of approximately all of the users of Ashley Madison, along with large amounts of internal documents and emails of the employees and executives of Defendants.

40. Rather than promptly inform members of the Class of the data breach, Defendants responded by misrepresenting when they first discovered the breach, downplaying the breach and providing a false sense of security to those Class members that happened upon the news through third party sources. On July 20, 2015, Defendant Avid Life Media issued an update on its website stating that "our team has now successfully removed the posts related to this incident as well as all Personally Identifiable Information (PII) about our users published online." This statement was misleading as it ignored the fact that the material was but a very small sample of the database to prove to Defendants the veracity of the data breach claim, and that the full database was still in possession of the Hacking Team who indicated they would publicly release and widely circulate the database under certain circumstances.

41. To the astonishment and dismay of the Class, the truth was far from that presented by Defendants in their July 20, 2015 response. With its announcement, the Impact Team had contemporaneously demanded that if Defendants did not shut down Ashley Madison the Impact Team would release the user database. Defendants failed to disclose such in their July 20, 2015 announcement, and also failed to subsequently counter-act the demands of the Impact Team. On August 18, 2015, the Impact Team released for public downloading and access the Ashley Madison user database containing the PII of the members of the Class. The data dump amounted to nearly 10 gigabytes of data and included, among other things, actual names, user names, addresses, phone numbers, email addresses, date of birth, credit card information, transaction

dates and amounts for purchases at Ashley Madison, and other sensitive information provided in filling out user profiles. The Impact Team has also subsequently released damning correspondence and internal documents from Defendants evidencing Defendants' awareness of the weakness of the security systems it had in place to protect the Class' PII.

42. Along with the release of the PII, members of the Full Delete Removal Subclass learned for the first time that the Full Delete Removal option and service marketed by Defendants had been misrepresented to the Class. The Full Delete Removal service and option was marketed to Plaintiff and the Class as an extra security measure by which Defendants would delete from their servers the user's PII and any additional traces of users' registration with Ashley Madison. Defendants marketed that users "can pay to eliminate any trace of themselves from the site" using the Full Delete option. The Full Delete Removal option represented in large font "Be Discreet, remove all traces of your usage for only $19.00" and invited users to "delete your profile." According to the item description displayed to Plaintiff and the Class, the "Full Delete Removal" purchase included among other things "removal of profile from the site" and "removal of site usage history and personally identifiable information from the site."

43. However, contrary to what was advertised and marketed, the Full Delete Removal option merely deleted some limited profile data and left stored on Defendants' servers significant amounts of PII sufficient to establish a users' identity and use of Ashley Madison. Instead of a full purging of the users' information and history on the site, the Full Delete Remove left substantial PII in Defendants' database including the users' email address, date of birth, date of creation of account, last update of account, account type, nickname of the account, city, state and country of the account holder, gender, ethnicity, a number of sexual preference categories, and their relationship status.

44. Because the Full Delete option and service did not perform the deletions expressed and implied by Defendants' marketing, Plaintiff and the Class members who purchased the Full Delete found their PII part of the data obtained and distributed by the Impact Team. Accordingly, the Full Delete option demonstrably failed to work as advertised. Had members of the Full Delete Subclass been aware that the Full Delete service did not completely eliminate the traces of their past registration and use of Ashley Madison they would not have purchased the Full Delete option.

45. Although Defendants had learned of the breach by at least July 19, 2015, Defendants did not make any adequate or prompt attempt to inform Plaintiff or the Class of the Data Breach. Finally, on August 19, 2015, Avid Life Media issued an update on its website merely indicating that it had "learned that the individual or individuals responsible for this attack claim to have released more of the stolen data." Defendants have not offered members of the Class any curative protection to assist the Class in preventing, addressing or curing the theft of users PII or attempts to extort users with the wide spread disclosure of the sensitive information contained in the database.

46. The security breach, and the failure to promptly discover and block the Data Breach, was the result of Defendants' grossly inadequate information systems and data security oversight. These failures enabled the perpetrators to obtain Class members' PII and subsequently use this information to steal from and extort members of the Class. Defendants' failures further put the Class members at serious risk of ongoing financial loss and identity theft, exposed the most sensitive, and embarrassing, information concerning their private lives to the world at large, and created irreparable harm.

47. While Defendants were enriched by its scheme through the monies it received from touting falsely the strength of its network security and the purported benefits of its "Full Delete" option, Plaintiff and the Class suffered damages as a result of each of their purchases of the Ashley Madison services because: (a) the services were not accompanied by the data security measures implied and expressly marketed by Defendants; (b) the information provided to Defendants necessary to obtain the services was not protected by the data security measures implied and expressly marketed by Defendants; (c) their private data was exposed so that it could be transferred and viewed by unauthorized third parties; (d) their PII, including users' addresses, phone number, email addresses and intimate preferences and practices, have been compromised and widely distributed publicly for the world to see creating irreparable harm; (e) they are exposed to a substantial risk of identity theft and related fraud; and (f) for the Full Delete Removal Subclass, the "Full Delete Removal" option and service did not provide the benefits implied and expressly marketed by Defendants.

48. As a result of Defendants' unreasonable and inadequate data security, Plaintiff were harmed by their registration for and acquisition of services offered by Defendants by being denied the value of what was marketed to Plaintiff.

49. Had Plaintiff and the Class members known of the true facts about Ashley Madison and the Full Delete Removal option they would either have not registered and made purchases from Ashley Madison, or would have not purchased the Products at inflated prices.

V. PLAINTIFF'S CLASS ACTION ALLEGATIONS

50. Plaintiff bring this lawsuit on behalf of themselves and the proposed Class members under Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure. Plaintiff seek certifications of classes defined as follows:

Nationwide Class
All persons and entities who registered with, or made purchases services from, the Ashley Madison website within the United States for the maximum period permitted by the statute of limitation applicable to each of the claims through July 15, 2015.

51. Pursuant to Fed. R. Civ. P. 23, Plaintiff also brings claims that the Company violated state consumer protection statutes on behalf of separate statewide classes in and under the respective consumer protection and data breach notice statutes. These classes are defined as follows:

Statewide Sub-Classes
All residents of [name of State or District of Columbia] who registered with, or made purchases from, the Ashley Madison website within the United States for a maximum period permitted by the statute of limitation applicable to the asserted state's consumer protection statute through July 15, 2015.

52. Excluded from each of the above Classes are Defendants, including any entity in which either Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by a Defendant, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of either of the Defendants. Also excluded are the judges and court personnel in this case and any members of their immediate families.

53. The Class comprises many thousands of consumers throughout New York and the United States. The Class is so numerous that joinder of all members of the Class is impracticable. There are questions of law and fact common to the Class. The common questions include:

a) Whether Defendants had adequate substantiation for the services' claims prior to making them;

b) Whether the claims by Defendants concerning the scope and performance of the Full Delete Removal service were true, or are misleading or reasonably likely to deceive given the limitations of the service;

c) Whether the Plaintiff were deprived of their bargain due to the limitations of the Full Delete Removal service as well as the inadequate security of the Ashley Madison servers and database;

d) Whether Class Members who paid for the Full Delete Removal service are due at a minimum, reimbursement for the failure of the Full Delete Removal service to perform as marketed and advertise and/or to prevent the dissemination of the PII of the Full Delete Removal Subclass members;

e) Whether Plaintiff and the Class are entitled to damages, civil penalties, punitive damages, declaratory and/or injunctive relief;

f) Whether there was an unauthorized disclosure by Defendants of Class members' personal and/or financial information;

g) Whether Defendants enabled an unauthorized disclosure of Class members' personal and/or financial information;

h) Whether Defendants misrepresented the safety and security of Class members' personal and/or financial information maintained by Defendant;

i) Whether Defendants implemented and maintained reasonable procedures and practices appropriate for maintaining the safety and security of Class members' personal and/or financial information;

j) When Defendants became aware of an unauthorized disclosure of Class members' personal and/or financial information;

k) Whether Defendants unreasonably delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;

l) Whether Defendants intentionally delayed notifying Class members of an unauthorized disclosure of Class members' personal and/or financial information;

m) Whether Defendants' conduct was negligent;

n) Whether Defendants' conduct was deceptive;

o) Whether Defendants' conduct was knowing, willful, intentional, and/or malicious;

p) Whether Defendants' conduct constitutes breach of an implied contract;

q) Whether Defendants engaged in deceptive acts and practices violating Section 349 of the New York General Business Law; and

r) Whether Defendants engaged in deceptive acts and practices violating Section 350 of the New York General Business Law; as alleged;

54. Plaintiff's claims are typical of the claims of the proposed Class, and Plaintiff will fairly and adequately represent and protect the interests of the proposed Class.

55. Plaintiff Does not have any interests antagonistic to those of the Class. Plaintiff has retained competent counsel experienced in the prosecution of this type of litigation.

56. The questions of law and fact common to the Class members, some of which are set out above, predominate over any questions affecting only individual Class members.

57. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it

impracticable or impossible for proposed Class members to prosecute their claims individually. The trial and the litigation of Plaintiff's claims are manageable.

58. Unless a class is certified, Defendants will retain monies received as a result of its conduct that was taken from Plaintiff and proposed Class members.

COUNT I
Violations Of State Data Breach Statutes
(On behalf of Plaintiff and the separate statewide data breach statute classes)

59. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

60. Legislatures in the states and jurisdictions listed below have enacted data breach statutes. These statutes generally require that any person or business conducting business within the state that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system to any resident of the state whose personal information was acquired by an unauthorized person, and further require that the disclosure of the breach be made in the most expedient time possible and without unreasonable delay.

61. Defendants' data breach constitutes a breach of the security system of the Company within the meaning of the below state data breach statutes and the data breached is protected and covered by the below data breach statutes.

62. Plaintiff's and Class members' names, credit and debit card numbers, card expiration dates, CVVs addresses, phone numbers and email addresses constitute personal information under and subject to the below state data breach statutes.

63. Defendants unreasonably delayed in informing the public, including Plaintiff and members of the statewide Data Breach Statute Classes ("Class," as used in this Count), about the

breach of security of Plaintiff's and Class members' confidential and non-public personal information after Defendants knew or should have known that the data breach had occurred.

64. Defendants failed to disclose to Plaintiff and Class members without unreasonable delay and in the most expedient time possible, the breach of security of Plaintiff's and Class members' personal and financial information when the Company knew or reasonably believed such information had been compromised.

65. Plaintiff and members of the Class suffered harm directly resulting from the Defendants' failure to provide, and the delay in providing, Plaintiff and Class members with timely and accurate notice as required by the below state data breach statutes. Plaintiff suffered the damages alleged above as a direct result of the Company's delay in providing timely and accurate notice of the data breach.

66. Had Defendants provided timely and accurate notice of the data breach, Plaintiff and Class members would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Defendants in providing notice. Plaintiff and Class members could have avoided making credit or debit card purchases on Ashley Madison, could have avoided utilizing the services of Ashley Madison at all, and could have contacted their banks to cancel their cards, or could otherwise have tried to avoid the harm caused by the Defendants' delay in providing timely and accurate notice.

67. The Defendants' failure to provide timely and accurate notice of the data breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), et seq.;

b. Ark. Code Ann. § 4-110-105(a), et seq.;

c. Ariz. Rev. Stat. § 44-7501, et seq.;

d. Cal. Civ. Code § 1798.83(a), et seq.;

e. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;

f. Conn. Gen. Stat. Ann. § 36a-701b(b), et seq.;

g. Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;

h. D.C. Code § 28-3852(a), et seq.;

i. Fla. Stat. Ann. § 501.171(4), et seq.;

j. Ga. Code Ann. § 10-1-912(a), et seq.;

k. Haw. Rev. Stat. § 487N-2(a), et seq.;

l. Idaho Code Ann. § 28-51-105(1), et seq.;

m. Ill. Comp. Stat. Ann. 530/10(a), et seq.;

n. Iowa Code Ann. § 715C.2(1), et seq.;

o. Kan. Stat. Ann. § 50-7a02(a), et seq.;

p. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;

q. La. Rev. Stat. Ann. § 51:3074(A), et seq.;

r. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;

s. Mass. Gen. Laws Ann. Ch. 93H § 3(a), et seq.;

t. Mich. Comp. Laws Ann. § 445.72(1), et seq.;

u. Minn. Stat. Ann. § 325E.61(1)(a), et seq.;

v. Mont. Code Ann. § 30-14-1704(1), et seq.;

w. Neb. Rev. Stat. Ann. § 87-803(1), et seq.;

x. Nev. Rev. Stat. Ann. § 603A.220(1), et seq.;

y. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;

z. N.J. Stat. Ann. § 56:8-163(a), et seq.;

aa. N.Y. Gen. Bus. Law §899-aa, et seq.; N.Y. State Tech. Law 208, et seq.;

bb. N.C. Gen. Stat. Ann. § 75-65(a), et seq.;

cc. N.D. Cent. Code Ann. § 51-30-02, et seq.;

dd. Okla. Stat. Ann. Tit. 24 § 163(A), et seq.;

ee. Or. Rev. Stat. Ann. § 646A.604(1), et seq.;

ff. Pa. 73 Stat. § 2301, et sq.;

gg. R.I. Gen. Laws Ann. § 11-49.2-3(a), et seq.;

hh. S.C. Code Ann. § 39-1-90(A), et seq.;

ii. Tenn. Code Ann. § 47-18-2107(b), et seq.;

jj. Tex. Bus. & Com. Code Ann. § 521.053(b), et seq.;

kk. Utah Code Ann. § 13-44-202(1), et seq.;

ll. Va. Code. Ann. § 18.2-186.6(B), et seq.;

mm. Wash. Rev. Code Ann. § 19.255.010(1), et seq.;

nn. Wis. Stat. Ann. § 134.98(2), et seq.; and

oo. Wyo. Stat. Ann. § 40-12-502(a), et seq.

68. Plaintiff and members of each of the statewide Data Breach Statute Classes seek all remedies available under their respective state data breach statutes, including but not limited to a) damages suffered by Plaintiff and Class members as alleged above, b) equitable relief, including injunctive relief, and c) reasonable attorney fees and costs, as provided by law.

COUNT II
Breach of Implied Contract
(On behalf of Plaintiff and the separate statewide breach of implied contract classes)

69. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

70. When Plaintiff and members of the Breach of Implied Contract Classes ("Class" as used in this Count) provided their PII to Defendants in order to make purchases at the Ashley Madison website, Plaintiff and members of the Class entered into implied contracts with the Defendants pursuant to which the Defendants agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

71. Defendants' solicited and invited Plaintiff and members of the Class to make purchases from Ashley Madison using their credit or debit cards. Plaintiff and members of the Class accepted the Defendants' offers and used their credit or debit cards to purchase items and services Ashley Madison during the period of the data breach.

72. Each registration of an account, and purchase made from Ashley Madison by Plaintiff and members of the Class using their credit or debit card, was made pursuant to the mutually agreed upon implied contract with the Company under which the Company agreed to safeguard and protect Plaintiff's and Class members' personal and financial information, and to timely and accurately notify them that such information was compromised and breached.

73. Plaintiff and Class members would not have provided and entrusted their financial and personal information to Defendants in order to utilize the services of, or make purchases from, Ashley Madison in the absence of the implied contract between them and the Company.

74. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Defendants.

75. Defendants breached the implied contracts it made with Plaintiff and Class members by failing to safeguard and protect the personal and financial information of Plaintiff

and members of the Class and by failing to provide timely and accurate notice to them that their personal and financial information was compromised in and as a result of the data breach.

76. The losses and damages sustained by Plaintiff and Class members as described herein were the direct and proximate result of Defendants' breaches of the implied contracts between Defendants and Plaintiff and members of the Class.

77. Wherefore, Plaintiff pray for relief as set forth below.

COUNT III
Bailment
(On behalf of Plaintiff and the separate statewide bailment classes)

78. Plaintiff reallege and incorporate by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

79. Plaintiff and members of the separate statewide Bailment Classes ("Class" as used in this Count) delivered their personal and financial information, to Defendants for the exclusive purpose of registering and creating a user account and profile at, and/or making purchases from, Ashley Madison.

80. In delivering their personal and financial information to Defendants, Plaintiff and Class members intended and understood that the Defendants would adequately safeguard their personal and financial information.

81. Defendants accepted possession of Plaintiff's and Class members' personal and financial information for the purpose of providing services to Plaintiff and the Class Members that resulted in enhanced value to Defendants, as well as accepting payment for purchases by Plaintiff and members of the Class at Ashley Madison.

82. By accepting possession of Plaintiff's and Class members' personal and financial information, Defendants understood that Plaintiff and Class members expected Defendants to

adequately safeguard their personal and financial information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

83. During the bailment (or deposit), Defendants owed a duty to Plaintiff and Class members to exercise reasonable care, diligence and prudence in protecting their personal and financial information.

84. Defendants breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' personal and financial information, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' personal and financial information.

85. Defendants further breached its duty to safeguard Plaintiff's and Class members' personal and financial information by failing to timely and accurately notify them that their information had been compromised as a result of the data breach.

86. Defendants failed to return, purge or delete the personal and financial information of Plaintiff and members of the Class at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

87. As a direct and proximate result of the Defendants breach of its duty, Plaintiff and Class members suffered consequential damages that were reasonably foreseeable to Defendants, including but not limited to the damages set forth above.

88. As a direct and proximate result of the Defendants breach of its duty, the personal and financial information of Plaintiff and Class members entrusted to Defendants during the bailment (or deposit) was damaged and its value diminished.

89. Wherefore, Plaintiff prays for relief as set forth below.

COUNT IV
Negligence
(On behalf of Plaintiff and the separate statewide negligence classes)

90. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

91. Defendants owed numerous duties to Plaintiff and members of the separate statewide Negligence Classes ("Class" as used in this Count). Defendants' duties included the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting personal and financial data in its possession;

b. to protect the Plaintiff and Class members' personal and financial data using reasonable and adequate security procedures and systems that are compliant with the PCI Security Standards Council standards and consistent with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the data breach.

92. Defendants owed a duty of care not to subject Plaintiff and the members of the Class, and their accompanying personal and financial data, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices. Defendants solicited, gathered, and stored Plaintiff's and the Class members' personal information and financial data to enhance its businesses' value and to facilitate sales transactions.

93. Defendants knew, or should have known, of the risks inherent in collecting and storing personal information and financial data and the importance of adequate security.

Defendants received warnings from within and outside the company that hackers routinely attempted to access such information without authorization. Defendants also knew about numerous, well-publicized data breaches by other websites and national retailers.

94. Defendants knew, or should have known, that its computer systems did not adequately safeguard Plaintiff's and the Class members' personal and financial data.

95. Because Defendants knew that a breach of its systems would damage millions of its customers, including Plaintiff and the Class members, it had a duty to adequately protect their personal Information and financial data.

96. Defendants had a special relationship with Plaintiff and the Class members. Plaintiff's and Class members' willingness to entrust Defendants with their personal information and financial data was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect its systems and the personal information and financial data it stored on them from attack.

97. Defendants own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their personal information. Defendants misconduct included failing to: (1) secure its internal network layout; (2) utilizing, and failing to patch, software knowing that it had known security vulnerabilities; (3) comply with industry standard security practices, (4) follow the PCI Security Standards Council standards, (5) encrypt the personal information and financial data; (6) employ adequate network segmentation, (7) implement adequate system and event monitoring, and (8) implement the systems, policies, and procedures necessary to prevent this type of data breach.

98. Defendants also had independent duties under state laws that required Defendants to reasonably safeguard Plaintiff's and the Class members' personal information and financial data and promptly notify them about the data breach.

99. Defendants breached the duties it owed to Plaintiff and Class members in numerous ways, including:

a. by creating a foreseeable risk of harm through the misconduct previously described;

b. by failing to implement adequate security systems, protocols and practices sufficient to protect their personal information and financial both before and after learning of the data breach;

c. by failing to comply with the minimum industry data security standards, including the PCI Security Standards Council standards, during the period of the data breach; and

d. by failing to timely and accurately disclose that their personal information and financial data had been improperly acquired or accessed.

100. But for Defendants' wrongful and negligent breach of the duties it owed Plaintiff and Class members, their personal information and financial data either would not have been compromised or they would have been able to prevent some or all of their damages.

101. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Defendants' negligent conduct. Accordingly, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT V
Unjust Enrichment
(On behalf of Plaintiff and the separate statewide unjust enrichment classes)

102. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

103. Plaintiff and members of the separate statewide Unjust Enrichment Classes ("Class" as used in this Count) conferred a monetary benefit on Defendants in the form of monies paid for the purchase of services from Defendants during the period of Defendants' data breach.

104. Defendants appreciate or have knowledge of the benefits conferred directly upon them by Plaintiff and members of the Class.

105. The monies paid for the purchase of services by Plaintiff and members of the Class to Defendants during the period of Defendants' data breach were supposed to be used by Defendants, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and members of the Class.

106. Defendants failed to provide reasonable security, safeguards and protection to the personal and financial information of Plaintiff and Class members and as a result, Plaintiff and Class members overpaid Defendants for the services purchased through use of their credit and debit cards during the period of Defendants' data breach.

107. Under principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and members of the Class, because Defendants failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal and financial information that they paid for but did not receive.

108. As a result of Defendants' conduct as set forth in this Complaint, Plaintiff and members of the Class suffered damages and losses as stated above, including monies paid for Defendants' services that Plaintiff and Class members would not have purchased had Defendants disclosed the material fact that it lacked adequate measures to safeguard customers' data and had Defendants provided timely and accurate notice of the data breach, and including the difference between the price they paid for Defendants' services as promised and the actual diminished value of their services.

109. Plaintiff and the Class have conferred directly upon Defendants an economic benefit in the nature of monies and profits received from sales and unlawful overcharges to the economic detriment of Plaintiff and the Class.

110. The economic benefit, including the monies paid and the overcharges and profits derived by Defendants and paid by Plaintiff and members of the Class, is a direct and proximate result of Defendants' unlawful practices as set forth in this Complaint.

111. The financial benefits derived by Defendants rightfully belong to Plaintiff and members of the Class.

112. It would be inequitable under established unjust enrichment principles in the District of Columbia and all of the 50 states for Defendants to be permitted to retain any of the financial benefits, monies, profits and overcharges derived from Defendants' unlawful conduct as set forth in this Complaint.

113. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by Defendants.

114. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendants traceable to Plaintiff and the Class.

115. Plaintiff and the Class have no adequate remedy at law.

116. Wherefore, Plaintiff pray for relief as set forth below.

COUNT VI
Violation of Section 349 and 350 of the New York General Business Law
(On behalf of Plaintiff, the New York Subclass and the Full Delete Removal Subclass)

117. Plaintiff Jane Doe realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

118. Plaintiff Jane Doe asserts Count VI on behalf of herself, the New York Subclass Subclass and the members of the Full Delete Removal Subclass (the "Class" as referred to in this Count).

119. Plaintiff Jane Doe and members of the Class were members of the "consuming public" for which the New York General Business Law ("NYGL") was intended to protect.

120. By their conduct described above, Defendants have engaged and continue to engage in deceptive acts and practices in the conduct of business, trade and commerce, and in the furnishing of services within New York State, all in violation of the New York General Business Law, § 349 et seq.

121. Section 349(h) provided in relevant part that:

> … any person who has been injured by reason of any violation of this section may bring an action in his own name to enjoin such unlawful act or practice, [and] an action to recover his actual damages …

122. Plaintiff and the Class members are "person[s] who have been injured" by reason of Defendants' violation of §349.

123. Section 350 of the New York General Business law makes unlawful "false advertising in the conduct of any business, trade or commerce or in the furnishing of any service in this state."

124. Defendants' act and practices described above have directly and proximately resulted in damages to Plaintiffs and Class members.

125. Defendants offered and advertised the Ashley Madison website as a secure website to provide their sensitive PII, as well as the Full Delete Removal service as being able to eliminate the traces of the users' past registration and use of Ashley Madison in order to induce the Plaintiff Jane Doe and members of the Class to register on the Ashley Madison website, provide sensitive PII to Defendants, make purchases of goods and services from Defendants, and make purchases of the Full Delete Removal service from Defendants. Defendants intended for Plaintiff Jane Doe and the other members of the Class to rely on Defendants to protect, secure, delete and prevent access from unauthorized third parties to PII furnished to it by Plaintiff Jane Doe and the Class in connection with their registration on Ashely Madison and purchases of goods and services made therefrom. Defendants further intended for Plaintiff Jane Doe and the Class to rely upon Defendants to institute and provide the services advertised and implied by the Full Delete Removal service when making the purchase of Defendants' Full Delete Removal service.

126. Plaintiffs and the other Class members relied upon Defendants' acts, statement, and omissions in order to utilize and/or purchase the services, credits, and/or Full Delete Removal service, each of which constitutes either "goods" or "services" within the meaning of the New York General Business Law.

127. Instead of a full purging of the users' information and history on the site as marketed and promised, Defendants knowingly, and intentionally, kept substantial PII in Defendants' insecure database. Compounding Defendants' inadequate oversight of its system and procrastination in curing the data breach, Defendants' acts and omissions eventually caused

the Full Delete Removal Class's PII to be hacked by Impact Team and caused tremendous emotional and financial damages to Plaintiff Jane Doe and the entire Full Delete Removal Subclass.

128. Besides Defendants' malicious deception to Jane Doe and the Class, Defendants also willfully failed to follow industry best practices concerning data theft or was negligent in preventing such data theft from occurring, and concealed, omitted and misrepresented this fact from Plaintiff Jane Doe and the Class.

129. Defendants benefited from taking no action to delete Plaintiff Jane Doe's and the Class' PII. Defendants further benefited from maintaining an insecure and susceptible database that exposed their customers' PII to theft by not having to make significant one-time and going expenditures to purchase, implement and maintain adequate measures that that would have prevented the data from being compromised, or limited the extent of the breach through early monitoring and detection.

130. Wherefore, Plaintiff prays for further relief as set forth below.

COUNT VII
Common Law Fraud
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Separate Statewide Classes)

131. Plaintiff realleges and incorporates by reference the allegations contained in the paragraphs above as if fully set forth here.

132. Defendants knowingly and/or recklessly engaged in the deceptive acts, uniform misrepresentations and material omissions complained of herein in order to induce Plaintiff and the Class members to register with Ashley Madison, purchase Defendants' services, including the purchase of credits and/or the Full Delete Removal service. Defendants utilized the same

deceptive acts to induce Class members to send their private data to Ashley Madison. Defendants

133. Plaintiff and the Class members relied upon Defendants' deceptive practices, uniform misrepresentations, and omissions.

134. As a result of Defendants conduct, Plaintiff and the Class have suffered damages in an amount to be determined at trial. Moreover, the imposition of punitive damages against Defendants is appropriate as the complained of conduct was malicious, willful, wanton and oppressive, or in reckless disregard of the rights of Plaintiff and the Class.

135. Accordingly, Plaintiff and the Class should be awarded restitution in the amount by which Defendants have been unjustly enriched, including, without limitation, all profits obtained by Defendants from its unlawful conduct.

COUNT VIII
Declaratory Judgment
(On behalf of Plaintiff and the Nationwide Class or, Alternatively, the Separate Statewide Negligence and Breach of Implied Contract Classes)

136. Plaintiff realleges and incorporates by reference every allegation set forth in the preceding paragraphs as though alleged in this Count.

137. As previously alleged, Plaintiff and members of the Breach of Implied Contract classes entered into an implied contract that required Defendants to provide adequate security for the personal information and financial data it collected from their credit and debit card transactions. As previously alleged, Defendants owes duties of care to Plaintiff and the members of the Nationwide class or, alternatively, the separate statewide Negligence classes, that require it to adequately secure PII and financial data

138. Defendants still possess the PII and financial data regarding Plaintiff and the

Class members.

139. After Defendants' data breach, Defendants announced changes that it claimed would improve data security. These changes, however, did not fix many of the systemic vulnerabilities in Defendants' computer systems.

140. Accordingly, Defendants still has not satisfied their contractual obligations and legal duties to Plaintiff and the Class members. In fact, now that Defendants' lax approach towards information security has become public, the personal information and financial data in Defendants' possession is even more vulnerable.

141. Actual harm has arisen in the wake of Defendants' data breach regarding its contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Breach of Implied Contract and Negligence Classes. Defendants maintain that their security measures now are adequate even though their changes are insufficient to meet Defendants' contractual obligations and legal duties. Plaintiff, therefore, seek a declaration (a) that Defendants' existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (b) that to comply with their contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to: (1) ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures; (4) ordering that

Defendants' segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendants is compromised, hackers cannot gain access to other portions of Defendants' systems; (5) ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services; (6) ordering that Defendants conduct regular database scanning and securing checks; (7) ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and (8) ordering Defendants to meaningfully educate its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Defendants' customers must take to protect themselves.

RELIEF SOUGHT

WHEREFORE, Plaintiff prays for relief and judgment pursuant to the claims as follows:

a. Determining that this action is a proper class action and certifying Plaintiff as class representatives under Rule 23 of the Federal Rules of Civil Procedure and Plaintiff's counsel as Class Counsel;

b. Awarding actual and compensatory damages in favor of Plaintiff and the other Class members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

c. Restitution and disgorgement of all amounts obtained by Defendants as a result of its unlawful activities, together with interest thereon from the date of payment, to the victims of such violations;

d. Awarding punitive damages in favor of Plaintiff;

e. An Order requiring Defendants to immediately cease its wrongful conduct; enjoining Defendants from selling, directly or indirectly, the Products through the use of false and misleading statements complained of herein; ordering Defendants to engage in a corrective notice campaign; and requiring Defendants to implement a full replacement program of all Products, or, in the alternative and at the preference of Plaintiff and each member of the Class, a refund for the purchased Products; and/or other equitable relief according to proof;

f. Awarding Plaintiff and the Class their reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees, and all applicable interest; and

g. Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: September 4, 2015

Respectfully submitted,
THE ROSEN LAW FIRM, P.A.

/s/ Phillip Kim

Laurence M. Rosen, Esq.
Phillip Kim, Esq.
275 Madison Avenue, 34th Floor
New York, New York 10016
Telephone: (212) 686-1060
Email: lrosen@rosenlegal.com
Email: pkim@rosenlegal.com

The Hinton Law Firm
Christopher S. Hinton
275 Madison Ave., 34th Floor

New York, NY 10016
Telephone: (646) 723-3377
Facsimile: (212) 202-3827
Email: chinton@hintonlegal.com

Attorneys for Plaintiff